REMARKS

The present application stands with claims 41, 47, 49-51, 59-61, 69-71, 77, 79 and 80 rejected under 35 U.S.C. §102(e) as being anticipated by the cited Brown et al. (Brown) patent. Claims 46, 56, 66, and 76 have been rejected under 35 U.S.C. §103(a) as being obvious over Brown and the cited Srivastava patent and claims 42-45, 48, 52-55, 58, 62-65, 68, 72-75, and 78 have been rejected under 35 U.S.C. §103(a) as being obvious over Brown and the cited Hawthorne patent. For the reasons below, the claims, as amended above, are believed to be neither anticipated by nor obvious over the cited references.

Applicants' have recognized, in accordance with their invention, that a device transmitting messages at a frequency that hops from frequency-to-frequency in a predictable pseudo-random manner can be tracked by an eavesdropper who is able to detect that hopping frequency pattern. Once that pattern is detected and the identity of the device determined, as the user of the device moves from location-to-location, the eavesdropper can track that user, thereby threatening his privacy and security. As described in the specification for the Bluetooth-enabled embodiment of the present invention, the hopping sequence of frequencies is determined as a predictable pseudo-random function of a universal time parameter and the BD_ADDR of the master Bluetooth device that is operating on the piconet on which the device is transmitting. As described, the BD_ADDR is a 48-bit word so that there are 2^{48} different BD_ADDRs, which each produce an associated hopping sequence. A computer-heavy eavesdropper could determine which hopping sequence is associated with a particular user by listening for signal energy in different bands and eventually determining the BD_ADDR associated with that device. Once the BD_ADDR is determined, the hopping sequence used by that device can be readily determined since it is derived from the universal time parameter and that

BD_ADDR. Thereafter, the location of that device and thus the user could be tracked by detecting that that hopping sequence is being used. Applicants have determined that the ability of an eavesdropper to track a device can be impeded by introducing a seed into the function that determines the hopping sequence from the universal time parameter and the device's BD_ADDR. This further randomizes that hopping sequence thereby making is more difficult for the eavesdropper to identify a device's BD_ADDR and track the device. By changing the seed over time, the eavesdropper will be severely impeded in his ability to track the device from the hopping sequence.

The Brown patent cited by the Examiner as disclosing that the hopping sequence is determined from a known function of the device identifier, a universal time parameter and a seed. Contrary to the Examiner's contention, however, Brown only discusses applicants' admitted prior art. There is nothing in Brown that indicates that "each frequency in the hopping sequence is determined from a known function of the particular identifier, the universal time parameter, and a seed that is changed over time and that further randomizes the hopping sequence from the predictable pseudo-random hopping sequence that which would otherwise be determined from the particular identifier and the universal time parameter alone." Brown discusses nothing about a seed that changes the sequence from that which would be determined from the time parameter and identifier alone. Brown states that "a pre-determined but pseudo random sequence of frequency hops is performed" (col 24, lines 52-53), but says nothing about being a function also of a seed that further randomized the hopping sequence. Reliance on Brown as being anticipatory of applicants' claimed invention is thus without merit.

The Examiner further contends that Hawthorne teaches an encryption/decryption apparatus that employs random seeds for security and that the seed is changed over time. What Hawthorne discloses is that a different random session key is used for each new session. In Hawthorne, however, the session key is used for encrypting the transmitted message. In applicants' invention, the message is not encrypted with different keys, or seeds. In fact, in applicants' disclosed embodiment, the message is not at all encrypted. In applicants' claimed invention the seed used to randomize the hopping sequence and it is that randomization of the hopping sequence that is changed over time. Changing the hopping sequence over time in applicants' invention does not in any way change the message and the ability of a receiver to decode it as does changing the random session key in Hawthorne. It is by further randomizing the pseudo random hopping sequence over time that is taught by applicants that advantageously inhibits a device from outside the predefined set of devices from determining the hopping sequence detected by an eavesdropper and from associating that sequence with a particular device within the set of devices. As a result, this prevents tracking of any particular device within the set by an eavesdropping and malevolently operated device outside the set, thereby keeping the user's privacy secure. Thus, changing over time a session key used to code a message cannot be properly analogized with changing over time a seed used to generate and further randomize a hopping sequence of frequencies as taught by the applicants.

For the reasons above, independent amended claims 41, 51, 61 and 71 are neither anticipated by nor obvious over the cited references and should accordingly be allowed. The dependent claims thereon should also therefore be allowed. Passage to issue of the subject application is therefore respectfully requested. Should the Examiner feel that the present application is not yet in a condition for allowance and that a telephone or personal interview would be helpful, he is invited to contact applicants' undersigned attorney at **973, 386 8252.**

Respectfully submitted,

Bjorn Markus Jakobsson
Susanne Gudrun Wetzel

By Stephen M. Gurey
Stephen M. Gurey
Attorney for Applicants
Reg. No.: 27336

Date: October 27, 2004

Docket Administrator (Room 3J-219)
Lucent Technologies Inc.
101 Crawfords Corner Road
Room 3J-219
Holmdel, New Jersey 07733-3030